Information Theoretic Security in Interference Networks

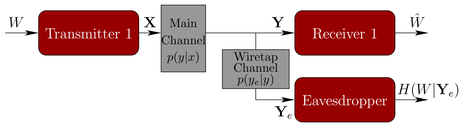
O. Ozan Koyluoglu and Hesham El Gamal (The Ohio State University)
Co-Authors: C. Emre Koksal, Lifeng Lai, and H. Vincent Poor

Abstract

Increasing demand in securing (wireless) networks has recently resulted in tremendous amount of research efforts in physical layer security. This work focuses on interference networks with secrecy constraints.

- For the two user channel, a scheme that allows users to cooperatively inject (decodable and undecodable) randomness is proposed. The results unveil the role of interference in secure network design.
- Next, the focus is shifted to arbitrarily high (but finite) number of users with asymptotically high signal to noise ratios. Utilizing the interference alignment scheme, a non-zero secure degrees of freedom is shown to be achievable at each user.
- Finally, random networks with large number of users is considered. Using tools from the percolation theory, a multi-hop scheme, where independent randomization is added at every hop, is shown to achieve the optimal scaling law under certain assumptions.

Information Theoretic Security in the Wiretap Channel



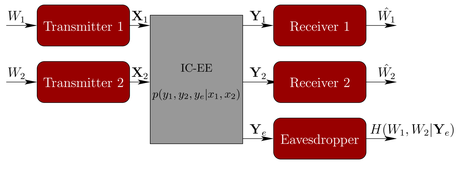
- Eavesdropper observes a degraded version of the output seen by the intended receiver.
- Coding technique [1] : Add extra randomness to the channel, so that the mutual information leakage rate to the eavesdropper $\frac{I(W;\mathbf{Y}_e)}{n}$ can be made arbitrarily small.

  1. Generate $2^{n(R+R^x)}$ codewords and partition them into 2^{nR} bins, where each bin contains 2^{nR^x} codewords.
  2. To send message w, choose a codeword in the bin w randomly and transmit the corresponding codeword denoted by $\mathbf{x}(w, w^x)$.
  3. Set the rates such that $R + R^x = I(X;Y)$ and $R^x = I(X;Y_e)$. This way, receiver recovers both the bin index (w) and the codeword index (w^x). Furthermore, the eavesdropper is totally confused due to this code design and the secrecy requirement is satisfied.

- The secrecy capacity is $C_s = \max_{p(X)} I(X;Y) - I(X;Y_e)$.

2-User Network: Cooperative Randomization

We assume that each transmitter $k \in \{1,2\}$ has a secret message $w_k \in \mathcal{W}_k \triangleq \{1, 2, \cdots, 2^{nR_k}\}$ which is to be transmitted to the respective receiver in n channel uses and to be secured from the external eavesdropper.



The error probability at the receivers are defined as follows.

$$P_{e,k} \triangleq \frac{1}{|\mathcal{W}_1||\mathcal{W}_2|} \sum_{(w_1,w_2)\in\mathcal{W}_1\times\mathcal{W}_2} \Pr\{\hat{w}_k \neq w_k | (w_1, w_2) \text{ is transmitted.}\}$$

We say that the rate tuple (R_1, R_2) is achievable for the IC-EE if, for any given $\epsilon > 0$, there exists a secret codebook such that,

$\max\{P_{e,1}, P_{e,2}\} \leq \epsilon \longrightarrow$ **reliability of the transmission**

$\frac{1}{n} I(W_1, W_2; \mathbf{Y}_e) \leq \epsilon \longrightarrow$ **secrecy of the transmission**

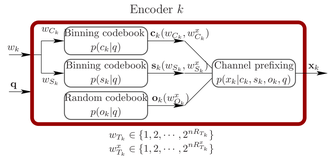
for sufficiently large n.

The proposed scheme allows for cooperation in adding randomness to the channel in two ways:

- **Cooperative binning $\longrightarrow$ To add structured and decodable randomness**
- **Cooperative channel prefixing $\longrightarrow$ To add unstructured and undecodable randomness**

Here, the binning technique of [1] and the channel prefixing technique of [2] are cooperatively exploited. The proposed scheme also utilizes the message-splitting technique of [3] to allow partial decoding of the interfering signals.

Random Variable	Codebook Type	Function
C_k	Binning codebook with rates R_{C_k} and $R^x_{C_k}$	Common information of transmitter k, will be decoded at both receivers
S_k	Binning codebook with rates R_{S_k} and $R^x_{S_k}$	Self information of transmitter k, will be decoded at receiver k and considered as noise at receiver $\{1,2\} - k$
O_k	Random codebook with rate $R^x_{O_k}$	Other information of transmitter k, will be decoded at receiver $\{1,2\} - k$ and considered as noise at receiver k



To probe further: The achievable region along with some special cases showing capacity and sum-capacity results can be found in [4].

References:

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[3] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inform. Theory*, vol. 27, no. 1, pp. 49-60, Jan. 1981.

[4] O. O. Koyluoglu and H. El Gamal, "Cooperative binning and channel prefixing for secrecy in interference channels," submitted. [Online]. Available at: arXiv.org.

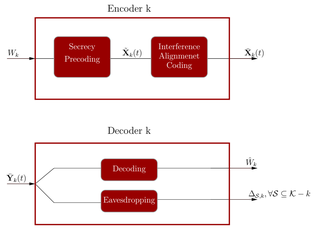
K-User Network: Secure Degrees of Freedom

We now focus on the frequency/time selective K-user Gaussian interference channel with secrecy constraints. Lets first consider the 3-user case with confidential messages.

1. Let $F = 2m+1$ for some m. This is the $(2m+1)$ symbol extension of the three-user channel considered in [5].
2. Employ interference alignment precoding using the matrices $\bar{\mathbf{V}}_k$ of [5], so that the transmitted signals are of the form $\bar{\mathbf{X}}_k(t) = \bar{\mathbf{V}}_k \tilde{\mathbf{X}}_k(t)$, where $\tilde{\mathbf{X}}_k(t)$ represents the vector of m_k streams transmitted from user k.
3. The F dimensional received signal space at each receiver is used to create m_i interference free dimensions, spanned by the desired streams.
4. Receiver 1 now sees the m streams $\tilde{\mathbf{X}}_2(t)$ and m streams $\tilde{\mathbf{X}}_3(t)$ mixed together in a multiple access channel with **only** m dimensions.
5. The secrecy precoding of $\tilde{\mathbf{X}}_2(t)$ and $\tilde{\mathbf{X}}_3(t)$ ensures to completely secure $m/2$ streams. In the limit of a large $F = 2m+1$, this results in 1/4 **secure DoF**.

The beamforming matrices $\bar{\mathbf{V}}_k$ satisfies the followings.

- **The non-intended signals seen by each receiver are aligned within some low dimensionality subspace.**
- **The intended streams span the orthogonal subspace.**



This intuitive discussion is formalized as follows. For the K-user Gaussian interference channel with confidential messages, a secure DoF of $\eta = \frac{K-2}{2K-2}$ per frequency-time slot is almost surely achievable for each user.

To probe further: The results are extended to the **external eavesdropper scenario**, where we design the scheme with a **virtual transmitter** corresponding to the eavesdropper, showing that the secure DoF of $\eta = \frac{K-1}{2K}$ is achievable. More interestingly, $\eta = \frac{1}{2} - \frac{1}{K}$ per user is achievable in the **absence of the eavesdropper CSI** by exploiting the channel ergodicity and permuting the users to assure symmetry. Details can be found in [6].

References:

[5] V. R. Cadambe and S. A. Jafar, "Interference Alignment and Degrees of Freedom of the K-User Interference Channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425-3441, Aug. 2008.

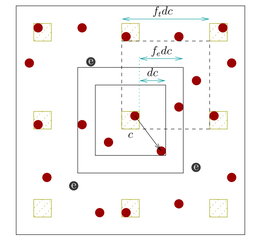
[6] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," submitted. [Online]. Available at: arXiv.org.

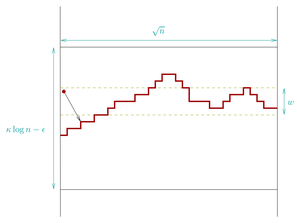
Large Networks: Secrecy Capacity Scaling

The network is on a square of side-length $\sqrt{n}$. The legitimate nodes and eavesdroppers are assumed to be placed randomly according to Poisson point processes of intensity $\lambda = 1$ and $\lambda_e = O\left((\log n)^{-2}\right)$, respectively. In such a network, we follow the footsteps steps of [7] to construct a highway backbone. However, in addition to the interference constraint considered in [7], our multi-hop forwarding strategy is designed to ensure secrecy.

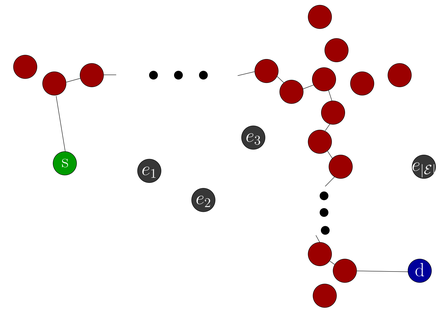
Our achievability argument is divided into the following four key steps:

1. **Secure rate per hop:** We first use the idea of **secrecy zone** to guarantee the secrecy of the communication over a single hop. **Key: Secrecy zone approach and bounding the interference on the legitimate receiver via time-division scheme.**
2. **Securing a multi-path:** Our novel multi-hop forwarding strategy, which injects independent randomization signal at each hop, is shown to allow for hiding the information from an eavesdropper which listens to the transmissions over **all** hops. **Key: Independent randomness injection.**
3. **Highway construction and secure rate per node on the highway:** Using tools from percolation theory, we show the existence of a sufficient number of horizontal and vertical highways. In particular, each highway is required to serve $O(\sqrt{n})$ nodes and an entry (exit) point has w.h.p. a distance of at most $\kappa' \log(n)$ away from each source (respectively, destination), where κ' can be made arbitrarily small. In addition, each node on the highway can support a constant data rate. **Key: Percolation with dependent edges.**
4. **Securing a multi-path:** Highways are shown to be accessible from **almost** all the nodes in the network with a secure rate of $\Omega\left((\log n)^{-3-\alpha}\right)$. **Key: Taking advantage of eavesdropper scaling.**





Our main result is then proved by combining the aforementioned steps with the following multi-hop routing scheme.



A typical multi-hop route consists of four transmission phases:

1. From source node to an entry point on the horizontal highway,
2. Across horizontal highway (message is carried until the desired vertical highway member),
3. Across vertical highway (message is carried until the exit node), and
4. From the exit node to the destination node.

The main result is as follows. If the legitimate nodes have unit intensity ($\lambda = 1$) and the eavesdroppers have an intensity of $\lambda_e = O\left((\log n)^{-2}\right)$ in an extended network, almost all of the nodes can achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$.

To probe further: Details can be found in [8], where we also show that the results also hold for **dense networks**. In addition, if nodes share keys only with the corresponding closest highway member, then **the same scaling is achievable for any $\lambda_e \to 0$.** More interestingly, the scaling result presented here is achievable even if the **eavesdroppers collude**.

References:

[7] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1009–1018, Mar. 2007.

[8] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On Secrecy Capacity Scaling in Wireless Networks," submitted. [Online]. Available at: arXiv.org.